

Raspodijeljene glavne knjige i kriptovalute

Anonimnost, skalabilnost i regulativa

Ante Đerek, Zvonko Konstanjčar

22. prosinca 2021.

S pozicije primjene

- Bitcoin primarno služi kao digitalni novac
 - Plaćanja
 - Prijenos kapitala
- Na Ethereum platformi možemo
 - Kreirati pametne ugovore
 - Kreirati digitalne novčiće (tokeni)

Glavni problemi proof-of-work sustava

- Ogromna potrošnja energije
- Rudarenje se svelo na nekoliko velikih bazena (ASIC) - sebično rudarenje

Ostali izazovi

- Anonimnost
- Skalabilnost
- Regulatoriva
- ...

Je li Bitcoin anoniman?

"Bitcoin is a secure and anonymous digital currency" - WikiLeaks donations page

"Bitcoin won't hide you from the NSA's prying eyes" - Wired UK

"Bitcoin Transactions Aren't as Anonymous as Everyone Hoped" - MIT Technology Review

Teška pitanja

- Želimo li kriptovalutu koja je potpuno anonimna?
- Je li anonimna kriptovaluta dobra za društvo?
- Možemo li zadržati samo pozitivne strane anonimnosti?

Doslovno: anonimno = bez imena

Dvije interpretacije

- Bez stvarnog imena
- Bez imena uopće

Bitcoin adrese su hashevi javnih ključeva.

Uobičajeno korištenje identiteta koji nije pravo ime nazivamo **pseudonimnost**.

Zašto anonimne kriptovalute?

Problem

- Kriptovalute zasnovane na lancu blokova su potpuno, javno i trajno sljedive
- Bez anonimnosti, privatnost je bitno manja nego kod tradicionalnih bankarskih sustava

Motivacija za anonimnim kriptovalutama

- Želimo razinu privatnosti kao kod klasičnih bankarskih sustava
- Želimo više razine privatnosti nego kod bankarskih sustava

Etika anonimnosti

- Postoji mnogo razloga za anonimnost - ne razmišljamo o njima kod bankarskih sustava
 - Želimo li da svi znaju našu plaću i na što trošimo novce?

Problemi s potpunom anonimnošću

- **Pranje novaca**
- **Kritična točka - ulaz i izlaz kapitala iz kriptovaluta**

Možemo li zadržati samo dobre strane?

- **Funkcionalnosti koje su moralno bitno različite**
- **Tehnološki su vrlo slične**

Definicija

Anonimnost = pseudonimnost + nepovezivost.

Korisnik je **anoniman** ako se njegove **različite interakcije** sa sustavom ne mogu **povezati**.

Primjer (anonimnost vs pseudonimnost): forum

- Komentiranje s identitetom
- Komentiranje bez identiteta

Zašto je važna nepovezivost?

Kod Bitcoina imamo pseudonimnost

- Lanac blokova je javan - svatko može pratiti svaku adresu
- Ako netko poveže stvarni identitet s adresom - zna sve transakcije te osobe

Povezivanje stvarnog identiteta s adresama je često lagano

- Mnoge Bitcoin usluge zahtijevaju stvarne identitete
- Povezani profili mogu se deanonimizirati kroz razne sporedne kanale

Ključna svojstva

- Trebalo bi biti teško povezati različite adrese istog korisnika
- Trebalo bi biti teško povezati različite transakcije istog korisnika
- Trebalo bi biti teško povezati platitelja i primatelja

Treće svojstvo je teško postići **direktno**.

Ideja: otežati povezivanje platitelja i krajnjeg primatelja.

Potpunu nepovezivost je teško postići

- Između svih transakcija
- Između svih adresa

Definicija

*Za danog napadača, **skup anonimnosti** (engl. *anonymity set*) određene transakcije je skup transakcija koje napadač ne može razlikovati od te transakcije.*

Za procjenu veličine skupa anonimnosti trebamo

- Definirati model napadača
- Definirati što napadač zna
- Definirati što napadač ne zna/ne može znati

Cilj je **maksimizirati** skup anonimnosti, tj. skup adresa i transakcija između kojih se možemo sakriti.

Generiranje puno različitih adresa

Bitcoin

Bitcoin is a secure and anonymous digital currency. Bitcoins cannot be easily tracked back to you, and are safer and faster alternative to other donation methods. You can send BTC to the following address:

384gapBnXX3UL756asn8HcBtindLoShJqd  

Various sites offer a service to exchange other currency to/from Bitcoins. There are also services allowing trades of goods for Bitcoins. Bitcoins are not subject to central regulations and are still gaining value. To learn more about Bitcoins, visit the website (<https://bitcoin.org>) or read more on [Wikipedia](#).

For a more private transaction, you can click on the refresh button above to generate a random **Segwit (BIP-49)** address.

Please **do not** use old (1HB5X...) donation address. ([message signed with old address here](#))



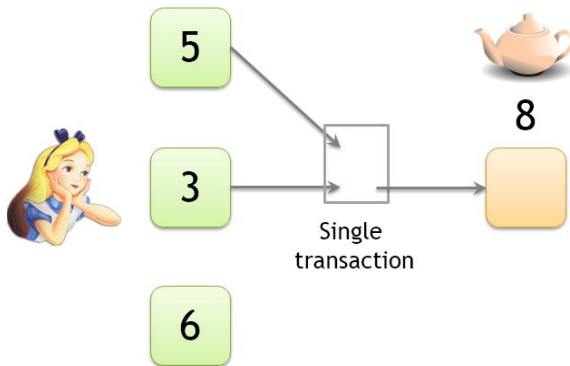
Izvor: shop.wikileaks.org/donate

Zadatak

Jesmo li postigli nepovezivost ako primamo Bitocine uvijek na druge adrese?



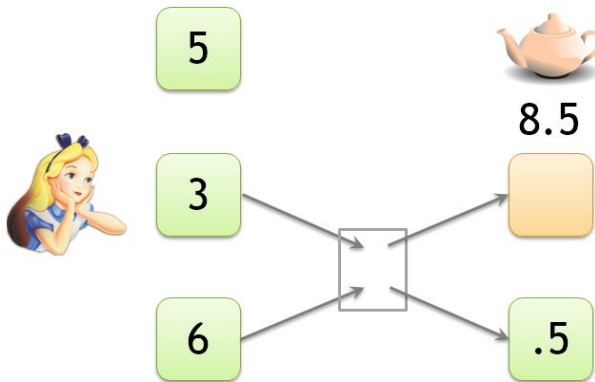
Ana kupuje čajnik



Izvor: bitcoinbook.cs.princeton.edu

- Zajedničko trošenje - ista kontrola
- Adrese možemo povezivati tranzitivno

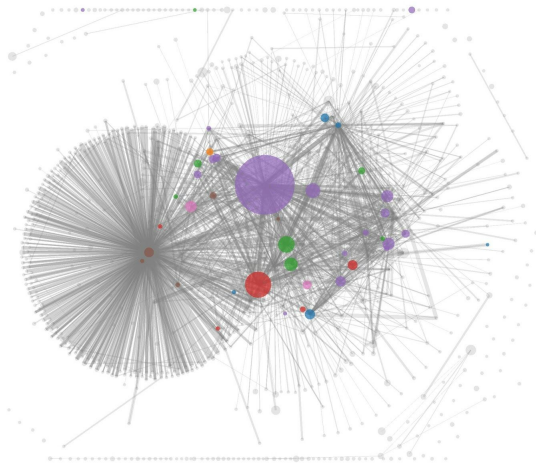
Ana kupuje čajnik - adresa ostatka



Izvor: bitcoinbook.cs.princeton.edu

- Adresu ostatka često definiraju novčanici - prilika za razne heuristike
- Jedna heuristika - adrese ostaka su nove

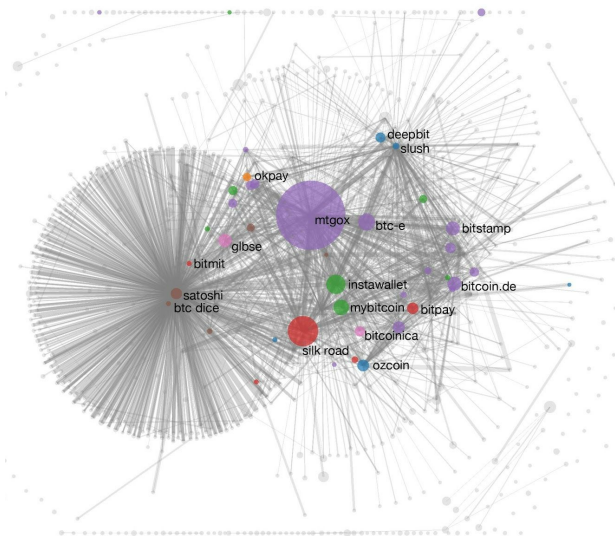
Zajedničko trošenje + heuristike = grupiranje adresa



Izvor: bitcoinbook.cs.princeton.edu

S. Meiklejohn, et al., A Fistful of Bitcoins: Characterizing Payments Among Men with No Names, 2013.

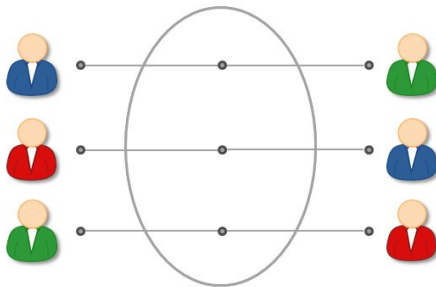
Označene grupe adresa



Izvor: bitcoinbook.cs.princeton.edu

Kako povećati anonimnost?

Direktno povezano s povećanjem nepovezivosti, tj. s otežanjem analize grafa transakcija.



Izvor: bitcoinbook.cs.princeton.edu

Jedno rješenje - tehnika koju nazivamo **miješanje**.

Intuicija: uvođenje posrednika povećava nepovezivost.

Online novčanici

- Pružaju usluge spremanja kriptovaluta online
- Novčići koje povlačimo nisu isti oni koje smo pohranili

Zadatak

Možemo li ostvariti efektivno miješanje kroz online novčanike?

Dobre strane

- Povećavaju "donekle" nepovezivost
- Otežavaju analizu grafa transakcija

Nedostaci

- Ne tvrde da će miješati sredstva korisnika
- I da miješaju, kod sebe drže zapise o tome
- Regulirani novčanici traže identitete osoba s kojima surađuju

Očigledno je anonimnost slična (vjerojatno manja) kao kod tradicionalnih banaka.

Je li nam to dovoljno?

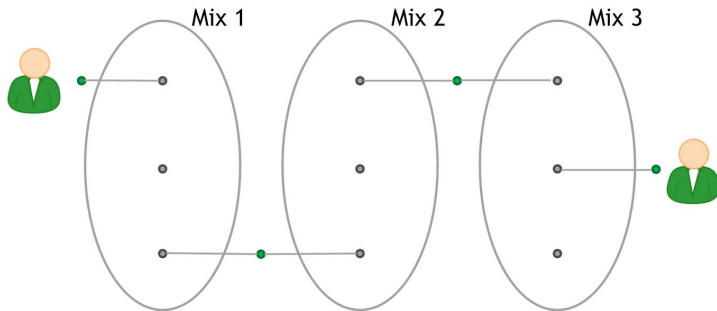
Svojstva

- Garantirano ne čuvaju zapise
- Ne traže identitet (niti username)
- Korisnik šalje Bitcoine i ciljanu adresu na adresu koju dobije od davatelja usluge miješanja
- Problematično **povjerenje u uslugu miješanja** - što ako ne rade što bi trebali?

Zadatak

Kako bi dodatno povećali anonimnost?

Usluge specijalizirane za miješanje - naprednija rješenja



Izvor: bitcoinbook.cs.princeton.edu

Svojstva

- Korištenje niza usluga miješanja
- Uniformne transakcije

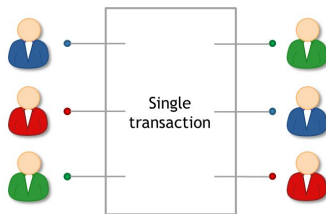
IDEJA: Zamijeniti uslugu miješanja s peer-to-peer protokolom pomoću kojeg grupa ljudi može miješati svoje novčiće.

Prednosti

- Korisnici ne moraju čekati davatelja usluge miješanja s adekvatnom reputacijom
- Krađa nije moguća u raspodijeljenom miješanju (osigurava protokol)
- Na neki način osigurava bolju anonimnost

Raspodijeljeno miješanje - združeni novčić (*engl. coinjoin*)

IDEJA: U ovom protokolu različiti korisnici stvaraju zajedničku transakciju koja kombinira sve njihove ulaze.



Izvor: bitcoinbook.cs.princeton.edu

Protokol - idejno rješenje

- Svaki korisnik dostavlja ulazne i izlazne adrese
- Poredak ulaznih i izlaznih adresa u tx se slučajno izmiješa
- Kada korisnici vide da je sve s njihovim iznosima i adresama u redu, potpisuju transakciju

Anonimnost - pregled rješenja

System	Type	Anonymity attacks	Deployability
Bitcoin	pseudonymous	transaction graph analysis	default
Manual mixing	mix	transaction graph analysis, bad mixes/peers	usable today
Chain of mixes or coinjoins	mix	side channels, bad mixes/peers	bitcoin-compatible
Zerocoin	cryptographic mix	side channels (possibly)	altcoin, trusted setup
Zerocash	untraceable	none known	altcoin, trusted setup

Izvor: bitcoinbook.cs.princeton.edu

Problemi

- Transakcije nisu trenutne
- Mikroplaćanja ne funkcioniraju - visoki transakcijski troškovi
- S porastom korisnika, funkcionalnost sve lošija

Transakcije u sekundi

- Bitcoin obrađuje oko 7 transakcija u sekundi (uz veličinu bloka 1MB i 250 bytes/tx)
- Trebalo bi biti dovoljno za čitav svijet?
- Visa obrađuje oko 2000 transakcija u sekundi (max 4000 tps)
- Uz 7 milijardi ljudi i prosječno 2 transakcije na mjesec, veličina bloka bi trebala biti 0.8 GB (5400 tps)

Izvor: <https://en.bitcoin.it/wiki/Scalability>

Veći blokovi = centralizacija

- Skupo validirati - malo punih čvorova
- Za veličinu blokova 1GB - za validaciju potrebni resursi na razini data centra - barijera za male čvorove
- Propagacija postaje problematična
- Stalna debata o tome kolika bi veličina blokova trebala biti

"Bitcoin itself cannot scale to have every single financial transaction in the world be broadcast to everyone and included in the block chain. There needs to be a secondary level of payment systems which is lighter weight and more efficient." - Hal Finney, Dec 2010.

A cypherpunk is any activist advocating widespread use of strong cryptography and privacy-enhancing technologies as a route to social and political change.

A Cypherpunk's Manifesto (Eric Hughes, 1993): "Privacy is necessary for an open society in the electronic age. ... We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy"

The technical roots of Cypherpunk ideas have been traced back to work by cryptographer David Chaum on topics such as anonymous digital cash and pseudonymous reputation systems, described in his paper "Security without Identification: Transaction Systems to Make Big Brother Obsolete" (1985).

Ideja

- Izuzeti male transakcije iz lanca blokova (izvan lanca, engl. off chain)
- Slično na burzama - transakcije bez izmjene na lancu blokova
- LN je općenitiji pristup

Primjer

- Ana ide na ručak redovito u Cassandru
- Neefikasno je koristiti lanac blokova za male transakcije
- Rješenje je uspostava multisig adrese dijeljene između Ane i Cassandre
- Multisig adresa je kao sef koji se može otvoriti samo ako se obje strane slože - "kanal plaćanja" (engl. "payment channel").

Primjer

- Kanal plaćanja se uspostavlja na lancu blokova
- Ana vidi svojih 0.03 BTC
- Cassandra vidi da Ana ima 0.03BTC na raspolaganju

Glavna knjiga kanala plaćanja, $t=0$

Ana (depozit)	0.03
Cassandra (depozit)	0

Primjer

- Ana ode na ručak u Cassandru, koji plati 0.001 BTC
- Glavna knjiga kanala plaćanja se osvježi (Ana i Cassandra imaju kopije)

Glavna knjiga kanala plaćanja, $t=1$

Ana	0.029
Cassandra	0.001

- Ana može ići na ručak u Cassandru, dok ne isprazni svoj račun
- Nema ograničenja na broj transakcija po sekundi, ove se transakcije odvijaju izvan lanca blokova

Zatvaranje kanala

- Kanal plaćanja se može zatvoriti u bilo kojem trenutku
- Bilo koji sudionik kanala plaćanja može poslati u mrežu posljednje stanje glavne knjige potpisano od svih sudionika
- Rudari validiraju potpise na glavnoj knjizi te ako je sve u redu raspodjeljuju sredstva

Važne karakteristike

- Jedine dvije transakcije na lancu blokova (i jedini troškovi) su kod uspostavljanja i kod zatvaranja kanala plaćanja
- Svatko može prekinuti kanal plaćanja, bez pristanka drugih
- Ivica ne treba uspostaviti kanal plaćanja prema Cassandri, ako ima uspostavljen kanal prema Ani, a Ana ima prema Cassandri.
- Mreža može pronaći najjednostavniji put kroz kanale plaćanja za obradu dane transakcije

Lightning network je protokol za plaćanje koji funkcioniра na aplikacijskom sloju koji se nalazi iznad lanca blokova.

Posljedice

- Ogromna brzina transakcija
- Niske naknade
- Moguće koristiti za mikro plaćanja

Lightning network je u produkciju krenuo 2018. godine.

Slično rješenje postoji na Ethereum lancu blokova - Raiden network.

Tko su dionici? Tko je glavni?

Core developeri

- Definiraju pravila
- Svi koriste njihov kod

Rudari

- Određuju koje transakcije su ispravne
- Grade povijest

Investitori, trgovci i korisnici

- Generiraju potražnju
- Određuju vrijednost valute

Za uspjeh kriptovalute - tri vrste konsenzusa

Konsenzus oko pravila

- Dogovor oko protokola i formata
- Što definira ispravnost transakcija, blokova

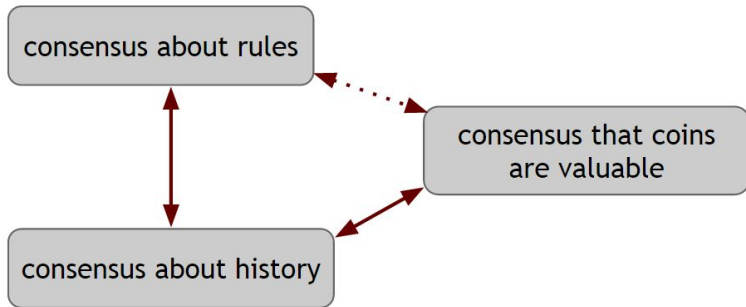
Konsenzus oko povijesti

- Dogovor oko sadržaja lanca blokova
- Koji novčići postoje i tko su njihovi vlasnici

Konsenzus oko vrijednosti

- Dogovor da novčići imaju vrijednost
- "Tinkerbell effect"

Za uspjeh kriptovalute - tri vrste konsenzusa



Izvor: bitcoinbook.cs.princeton.edu

Kontrola kapitala


- Iznošenje kapitala izvan države - postoje pravila i zakoni
- Trud usmjeren na odsijecanje (reguliranje) fiat valuta od kripto valuta

Kriminal

- Olakšavaju neke vrste kriminala, npr. plaćanje otmičarima, CryptoLocker, itd.
- Porezne prijevare su znatno lakše

Browser tabs: Welcome! | Silk Road | State of the Road Address | +


Address bar: silkroadvb5plz3r.onion



Silk Road


anonymous marketplace

messages(0) | orders(0) | account(\$0.00) | settings | log out

search |  (0)

Shop by category:


- Drugs(1582)
 - Cannabis(271)
 - Dissociatives(33)
 - Ecstasy(217)
 - Opioids(106)
 - Other(65)
 - Prescription(274)
 - Psychedelics(306)
 - Stimulants(190)
- Apparel(37)
- Art(1)
- Books(300)
- Computer equipment(9)
- Digital goods(218)
- Drug paraphernalia(33)
- Electronics(13)
- Erotica(165)
- Fireworks(1)
- Food(1)
- Forgeries(34)
- Hardware(1)
- Home & Garden(5)
- Lab Supplies(5)
- Medical(3)
- Money(89)
- Musical instruments(2)




10 Grams high grade MDMA 80+%
\$61.17

CC(N)Cc1ccccc1


Amphetamines sulfate / Speed freebase...
\$28.59




2g Jack Frost (weed) *420 SALE****
\$8.54




5 Grams of pure MDMA crystals
\$42.04




100 red Y tablets 111mg (lab tested)...
\$97.77




Michael Jackson Discography 1971-2009...
\$2.52



3.5g Albino Rhino (weed)
\$12.37



10mg Flexeril (muscle relaxant)...
\$3.22



***10gr. Amphetamine Sulphate...
\$33.19

News:

- The gift that keeps on **giving**
- Who's your **favorite**?
- Acknowledging **Heroes**
- A new anonymous market **The Army!**
- State of the Road Address**

Izvor: bitcoinbook.cs.princeton.edu

Veliki dio zagovaratelja kriptovaluta je protivnik regulative.

Česti negativni argumenti

- Regulativu pišu i provode birokrati koji ne razumiju poslovanje
- To je (nepotrebno) trenje u sustavu koje ne ispunjava svoju svrhu

Glavni pozitivni argument

- Kada tržišta ne funkcioniraju i rezultiraju ishodima koji su loši za veći dio sudionika tržišta tada regulacija potencijalno može popraviti ishode.
- Tržišta ne rezultiraju ishodima koji su uvijek dobri za većinu sudionika tržišta (pogotovo u kratkom roku)
 - Postoji bolja alokacija sredstava od postojeće prema kojoj će svi imati više ili barem jednako kao kod postojeće alokacije (Paretovo poboljšanje)

Primjer: nefleksibilne cijene (*engl. sticky prices*)

- Termin u ekonomiju uveo John Maynard Keynes
- Prema teoriji slobodnog tržišta radnici će uvijek biti spremni sniziti zahtjeve na svoje plaće na one razine na kojima će poslodavci moći njima ponuditi radna mjesta.
- U stvarnosti radnici često odbijaju sniziti zahtjeve na svoje plaće, čak i u slučajevima kada bi to bilo racionalno za njih.
- Interakcija agregatne ponude i potražnje vodi u stabilnu ravnotežu nezaposlenosti.

Primjer: tržište "limuna"

- George A. Akerlof, Michael Spence, Joseph E. Stiglitz - Nobelova nagrada 2001. godine
- Na tržištu imamo dva tipa proizvoda: kvalitetni i manje kvalitetni
- Ukoliko bi kupci bez problema i dodatnih troškova mogli utvrditi kvalitetu proizvoda tada bi tržište funkcioniralo - razlike u cijenama bi odražavale razlike u kvaliteti proizvoda
- Ako kupci ne mogu utvrditi razliku u kvaliteti, tada oni nemaju racionalnih razloga za kupnjom skupljeg proizvoda
- Proizvođači nemaju razloga proizvoditi skuplji proizvod
- Rezultat je stabilna ravnoteža u kojoj se proizvodi samo jeftiniji i manje kvalitetni proizvod
- Ovaj ishod je lošiji od ishoda efikasnog tržišta za gotovo sve sudionike tržišta

Tržište limuna (problematične su asimetrične informacije)

Bilo koji proizvod "widget" na tržištu koji pati od asimetričnih informacija (bilo kupci ili proizvođači imaju puno bolje informacije o kvaliteti proizvoda) može rezultirati s neuspjehom tržišta.

Popravci - tržišni

- Reputacija prodavača
- Garancije

Popravci - regulatorni

- Regulatori zahtijevaju objavljivanje informacija o kvaliteti
- Regulatori uspostavljaju standarde kvalitete
- Regulatori zahtijevaju od svih prodavača izdavanje garancija i nadziru reklamacije

Tajni sporazumi i zakon o tržišnom natjecanju

- Tržišta ne funkcioniraju kada se cijena proizvoda fiksira
 - Različiti prodavači se udružuju kako bi digli cijene (ili ih ne žele spustiti)
- Tržišta ne funkcioniraju kada ljudi poduzimaju akcije kojima sprječavaju tržišno natjecanje
 - Prodavači koji bi trebali biti konkurenti se dogovore o (ne)natjecanju

Ovakva ponašanja su nelegalna u većini nacionalnih zakonodavstava
- zakon o tržišnim natjecanjima.